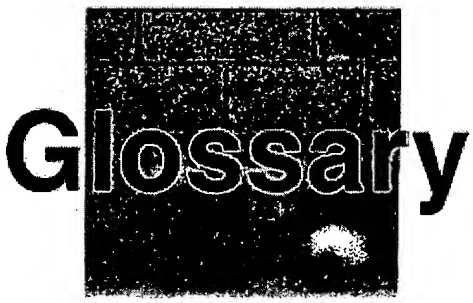
ACCdotcom home

GLOSSARY OF NETWORKING TERMS



This Glossary of Telecommunications and Internetworking Terms has been compiled for your reference by ACCdotCom

Your comments, corrections or additions are invited. Mail them to: info@accsystems.com

GO TO A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- **ACD (Automatic Call Distribution/Distributor)** A specialized phone system, or the service it provides, for handling many incoming calls. Typically used by airlines and hotels, it recognizes and answers incoming calls according to instructions in a database, before sending the call to an operator or agent. It also offers management information on the type and volume of calls and efficiency of the agents.

- **ACF/NCP (Advanced Communication Function/Network Control Program)** In host based IBM SNA networks, it is the control software running on a communications controller that supports the operation of the SNA backbone network.

- **ACF/VTAM (Advanced Communication Function/Virtual Terminal Access Method)** In host-based IBM SNA networks, it is the control software running or a host computer that allows the host to communicate with networked terminals.

- **Actius (Association of Computer Telephone integration Users and Suppliers)** A UK forum for users and suppliers to increase awareness of the business benefits of CTI. Act us develops education programs and information campaigns on CTI.

- **Address** One or a group of characters specifying the recipient or originator of transmitted data. An address car also denote the position of data in computer memory or the data packet itself while in transit through a network. IEEE 802.3 and 802.5 recommend having a unique address for each device worldwide.

- **ADPCM (Adaptive Differential Pulse Code Modulation)** A ITU-TS standard technique for voice encoding and compression. It allows an analog to be carried within a 32Kbit/s digital channel.

- **Adjusted Ring Length** When a segment of Token Ring (in practice a dual ring) trunk cable fails, a function known as the Wrap connects the main path to the backup path. In the worst case - the longest path - would occur if the shortest trunk cable segment tailed, so ARL is calculated during network design to ensure the system will always work.

- **Agent** A software-driven process running on a communications or networking device that allows that device to participate in a network management system. For example, an SNMP agent running on a router provides the ability for the router to exchange information with an SNMP network management system through the use of the SNMP protocol.

block of data is calculated before it is sent, and is then sent along with the data. A new CRC is calculated on the received data. If the new CRC does not match the one that has been sent along with the data then an error has occurred.

- **Cross-Connect** An ATM switch usually comprising three functional areas. System control The central control unit, which also provides the management interface of the system; the ATM "fabric block" providing the system switching capacity; termination groups to provide the external interfaces and the functions of the ATM layer of the network node. Each of these functional system areas is configured according to the specified needs of the respective network node. Each functional area usually has its own monitoring and control units for safeguarding the high availability of the complete system.

- **Crosstalk** Unwanted interference from another adjacent communications channel . The signal from the adjacent channel is inserted into the original communications channel.

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** The access method used in Ethernet. All nodes are attached to a single cable and contend equally for access to the transmission medium. if two nodes attempt to send data at the same time, they "sense" each other's signal and immediately stop sending. They will both try to send again after Waiting a random number of microseconds.

- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** A method of network access not covered by OSI standards and used in AppleTalk networks.

- **CSU (Channel Service Unit)** (1) In the US, data transmission equipment to repeat the signal from the carrier and ink to CPE. Vendors add value to CSUs by adding performance monitoring and management. (2) In Europe, CSUs are sold for their value features like diagnostics and performance monitoring. The basic repeating function is prd in the NTU (networking terminating unit). CSUs monitor quality on EI, E2 or E3 circuits in terms of transmission and line loading.

- **CT1** First generation analog domestic cordless telephone (non-cellular).

- **CT2** Two-way digital cordless telephony technology, particularly relevant to cordless PBXs. In its public guise, it becomes a one way telepoint service now no longer available in the UK but prevalent in the Far East.

- **CT3** Ericsson's proprietary cordless telecommunications system.

- **CTI (Computer Telephone Integration)** A generic name for the technology automatically relating computers and PABXs via applications such as ACD, power dialing, IVR and other customer facing or agent facing services. A so known by older, proprietary names CIT (Computer Integrated Telephony) and CSTA (Computer Supported Telephony Applications).

D

- **Darpa (Defense Advanced Research Projects Agency)** Formerly called Arpa, this US government agency that funded research and experimentation with the Arpanet and later, the connected Internet- The group within Darpa responsible for the Arpanet is ISTO (information Systems Techniques Office), formerly IPTO (Information Processing Techniques Office).

- **Dassill** A message based signaling system following the ISO based model developed by BT to provide multi-line IDA interconnection to the BT network.

- **Data compression** A way of reducing the amount of data to be transmitted by applying one of severs techniques that reduce the number of bits needed to represent the information. When the data is received It is decompressed into its original form.

- **Database server** A database installed as a back-end or server component of a client-server system, which can be accessed over a LAN by one or more client, or front-end applications through the use of query language, typically SQL. The server part of the program is responsible for updating the records, ensuring that multiple access is available to authorized users, protecting the data and communicating with other servers holding relevant data. The

client end of the program requests records and then modifies them, while the server tracks records down for the client and adds new ones.

- **Datagram** A method of sending data in which parts of the message are sent in random order. The recipient machine has the task of reassembling the parts in the correct sequence. The datagram is a connectionless, single packet message or item of data that can traverse a network at OS I Level Three, the Network Layer. It typically does not involve end-to-end session establishment or delivery-confirmation acknowledgment. As well as the information within the datagram, there is a destination network address and usually a source network address.

- **Data link** A direct serial data communications path between two devices without intermediate switching nodes.

- **Data Link Layer** Layer Two of the ISO OSI model is responsible for the transmission of information over a physical medium. After establishing the link it ensures the error-free delivery of the information through the use of error detection, error recovery and flow control. The contention access methods such as CSMA/CD and Token passing are Layer Two activities.

- **Data PBX** A switching system for data traffic that allows terminals and workstations connected by individual cables to the Data PBX selectively to link to one or more host computers over asynchronous circuits through the use of contention.

- **DCA (Defense Communication Agency)** The US government agency responsible for the installation of Defense Data Networks, like Arpanet and Milnet, and PSNs. The DCA writes contracts for operation of the DDN and pays for network services.

- **DCA (Document Content Architecture)** The IBM approach to storing documents as two types of document group: draft documents and final form documents. For presentation, the draft document is transformed into a final document through an office system.

- **DCE (Data Circuit Terminating Equipment)** Communications equipment installed in a user's premises responsible for establishing, maintaining and terminating a connection. A modem is an example.

- **DCE (Distributed Computing Environment)** A suite of software utilities and operating system extensions that will, in theory, create applications on networks of heterogeneous hardware - PCs, Unix workstations, minicomputers and mainframes. The DCE is the product of the OSF. The DCE is designed to simplify the building of heterogeneous client/server applications and provides seven general services: Remote Procedure Call, Security, Naming (directory), Distributed File System, Threads, Time and PC Integration. DDE (Dynamic Data Exchange) - A Microsoft messaging specification. When DDE-compliant applications are combined, dynamic documents can be created which update each other as data changes.

- **DDM (Distributed Data Management Architecture)** An IBM SNA LU 6.2 transaction providing users with facilities to locate and access data in the network. It involves two structures: DDM Source, and DDM Target. The Source works with a transaction application to retrieve distributed data and transmits commands to the Target program on another system where the data that has been requested is stored. The Target interprets the DDM commands, retrieves the data and sends it back to the Source that originated the request.

- **DDCMP (Digital Data Communication Message Protocol)** The DecNet- specific Link Level protocol that operates at Layer Two of the Digital Network Architecture.

- **DDN (Defense Data Network)** Used generally to refer to Milnet, Arpanet and the TCP/IP protocols those networks use. More specifically refers to Milnet and associated parts of the connected Internet that connect military installations.

- **DecNet** Proprietary peer-to-peer network technology originally developed for use in wide area networking by the Digital Equipment Corporation (Dec) and evolved to include significant Ethernet-based LAN capabilities. It is the implementation of the Digital Network Architecture (DNA).

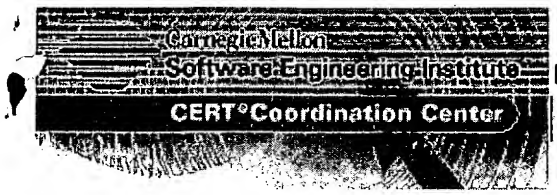
- **Dect (Digital European Cordless Telecommunications)** A standard governing pan-European digital mobile telephony. Based on advanced TDMA technology, Dect covers cordless PBXs, telepoint and residential cordless telephony.

- **X.520** Selected attribute types.
- **X.521** Selected object types.
- **Xapia (X.400 Application Programming Interface Association)** Body standardizing the interface to X.400 e-mail services. Other APIS, like VIM and MAPI, are likely to comply with Xapia when it is finalized.
- **X/Open** A body comprising of computer vendors, responsible for researching, defining and publicizing open systems.
- **X.Windows** A networked GU I based on a client/server architecture, it displays information from multiple networked hosts on a single workstation. Available on PCs as X.terminal emulation and emulation on LAN servers.

Y

Z

Send Information Return to Homepage



Install firewall hardware and software.

A practice from the CERT® Security Improvement Modules

Install and configure the operating system that will execute the firewall software followed by installing and configuring the firewall software. These two steps should be performed on the firewall hardware you intend to use in your production environment but deployed in the test environment and configuration (Refer to "8. Test the Firewall System" for information on using a test configuration). You need to ensure that all hardware and software are properly configured and operate as expected to the extent possible in the test configuration.

You need to configure the operating system on your firewall host in the minimum essential configuration so that only those services necessary for firewall operation and maintenance are included. You need to include all applicable patches or fixes for both the operating system and the firewall software.

Why this is important

The most common cause of firewall security breaches is misconfiguration of the firewall system. Various references on penetration testing show that well over half of the firewall systems regularly tested are not properly configured. According to ICSA[1], seventy percent of sites with certified commercial firewalls are still vulnerable to attacks due to misconfiguration or improper deployment.

Exercising your installation and configuration procedures in a test environment will allow you to learn the requirements to efficiently install and configure both the operating system and your firewall software while minimizing the impact on your operational systems. It will highlight what, if any, hardware may be missing in your initial configuration.

If you do not install the operating system and your firewall software with a minimal service configuration and with all applicable patches, you risk

- exposing your organization's network to intrusions that exploit well-known vulnerabilities for which patches exist
- not being able to get support from your vendor. Vendors almost always require the underlying system to be current before they will answer questions.
- not having a stable platform on which to run the firewall software. Many patches are related to reliability and recovery.

How to do it

Install a minimum acceptable operating system environment

Ensure that your firewall system configuration includes only those packages and services that are required for firewall system operation. This can be accomplished by either

- removing all software that is not needed (if this can be determined) after installation, or
- including only that software which is needed, selectively adding specific packages and services back in as you determine that they are required

Examples of services that are typically included in a default operating system configuration that should be removed are X Windows services, telnet (assuming ssh is installed and configured), NFS for Unix-based operating systems, and NetBios for Microsoft NT operating systems.

For some firewall products, the process of installing the firewall software will force a minimal configuration of the operating system such as removing unnecessary services if you did not do this before the installation process.

Keep in mind that packet filtering functions typically run in the operating system kernel (for performance reasons) and, therefore, packet filtering software is fairly sensitive to a specific kernel version and release number.

Once you are satisfied that the operating system and the firewall software is successfully installed, you should repeat the sequence to ensure that the process can be done again. The second time, document it. The third time, have an outside person who was not involved in the first two installations follow the documentation to see if it is correct and complete.

Take appropriate steps to ensure that any redundant systems are in a state consistent with the systems to be used in production. Ensure that you can easily switch between your primary firewall system and any redundant systems.

Your installed environment may not have all of the necessary troubleshooting and support tools necessary to determine what has happened if anything goes wrong during the installation process. You may need to install the firewall system on another host that has better diagnostic tools if you run into problems. After you understand the problems and know how to compensate for them, you can complete the installation on the production hardware.

Install all applicable patches

This information is available from your operating system and firewall software vendors. Determine how to deliver patches securely to the firewall system. Some products require that you do this using removable media (disk, CD-ROM), not via a network.

As an operational consideration, if your redundancy requirements result in your having an identical hot backup or standby firewall system (which we strongly recommend), you can consider installing and testing any new patches on the redundant system and then switch from the current operational system to the redundant system.

Your vendor service level agreement should state that the firewall software will always be fully functional if all of the operating system patches are installed.

In addition, you need to ensure that those responsible for your firewall operating system and software have time set aside to periodically review applicable public and vendor information sources for security patch updates. These sources regularly report current intruder trends, new attack scenarios, security vulnerabilities, methods for their detection, and guidance to address them.[2]

Restrict user and host access

The only users who should have access to your firewall system are the firewall system administrator, those authorized by policy, and individuals involved in operating and maintaining your information technology infrastructure.

For some firewall products, the process of installing the firewall software will automatically disable access to the firewall system by all users (except those mentioned above) if you have not already disabled their access before installation.

We recommend that you allow remote access to your firewall system only via mechanisms that

are strongly authenticated and strongly encrypted, even on your organization's internal networks. Some firewall products provide the capability to restrict the administrative client to a specific IP address and a specific port. We do not believe that this is adequate security; encryption is required as well. IP addresses and ports are too easily spoofed.

Disable IP forwarding

Make sure packet forwarding is disabled until after the firewall software is operational.

While booting firewall hosts, there may be an interval of time after the operating system is functional, including networking, but the firewall software is not yet functional. During this interval, packets may flow freely through the firewall system. Make sure that no packets are forwarded before the firewall software is functioning by doing one or more of the following

- disable IP routing before any interfaces are enabled
- do not enable network interfaces before the firewall software is functional

Backup your system

When installation is complete, perform a backup of the entire firewall system. Use this backup to restore the production system (or one identical to the test firewall system) for operation. Verify that both the operating system and the firewall software operate properly from the restored backup version. Refer to *Securing Desktop Workstations* [Simmel 99], specifically the practice "Configure computers for file backups."

Policy considerations

Your organization's networked systems security policy should require

- timely evaluation, selection, and installation of patches and other corrections that you need to operate securely
- that only authorized personnel have access to the firewall system via authorized, strongly authenticated mechanisms
- that firewall system installation is performed in an environment isolated from your operational networks
- that your firewall system is backed up on a regular basis

Footnotes

1. January, 1999 quote
2. A list of information sources can be found at the end of the Executive Summary of this module and at http://www.cert.org/security-improvement/implementations/i040.01.html, titled "Maintaining currency by periodically reviewing public and vendor information sources."

Back to top | Full list of modules, practices, and implementations

---

This page was last updated on July 1, 1999.

John Stenzel's Network Glossary

NOTE: This has been (and continues to be) a work in progress, constantly being updated and corrected. It started as a glossary and is becoming a primer for learning the vocabulary and concepts of networking at UCD, so that administrators and users in the English Department could make intelligent choices about networking (and UCD's Network 21 upgrades) as we planned our move Voorhies Hall. Thank-yous to Andy Austin, B.C. Cooper, Tim Leamy, Joe Aimone, Jessica Mignone and others for suggestions and guidance.

The alphabetical order is not ideal, since every term seems to be defined using other terms that need to be defined, but this is a start. Subsequent versions of this glossary will be hypertext-enhanced, with defined terms linking to other defined terms. Please address questions, comments, and requests for clarification to John Stenzel, jastenzel@ucdavis.edu. I have offered this document to various entities in our IT division, but so far they have not found it useful to change from their rather more skeletal resources. I believe the field desperately needs a more readable guide to these terms and principles, and would appreciate any suggestions you have, or to hear from you if you found it useful at all.

This update made June 6, 1997.

10BASE-T: Shorthand for 10 million bits per second (10 Mbps) line, like that currently joining Ethernet units on campus. The name comes from 10 for the 10-Megabits, BASEband transmission, on Twisted pair wire. That last is significant because twisted-pair wiring is much cheaper than coaxial cable; within buildings this is beefy wiring alongside phone cable.

10BASE-T Card and cabling: communications hardware (some of it inside the desktop computer and also the cabling) needed to join a computer to the NAM (Network Access Module) wall outlet and thence (via local hub and routers) to the Network 21. aka Network Adapter Card. Most new computers are Ethernet-ready out of the box, but retrofitting an older machine cost around $80-100 in 1996.

100BASE-T: the next generation of Ethernet communications gear, able to carry data at 100 million bps, ten times faster than 10BASE-T and about 100 times faster than regular fast modems.

address: a slippery term, depending on context; in e-mail world, the combination of usercode/mailname and domain designation allowing proper routing of messages to an individual (e.g., fzbozo@peseta.ucdavis.edu or jbozoclown@ucdavis.edu). In a network context, an address is the end of a glorified phone jack (a Network Access Module or NAM), able to be designated to receive packets of data in IP (Internet Protocol) form. All Internet traffic is tracked and routed by IP addressing, whether or not the addressing is manifest to the naked eye: the text address fzbozo@peseta.ucdavis.edu silently incorporates the four-digit IP address of the server known as peseta.ucdavis.edu. The number of IP addresses on a given subnet is limited by the number of ports served by the equipment in a given IDF closet.

AppleTalk: networking scheme (or protocol) developed by Apple allowing Macs to share a printer or network resources; runs 230 Kilobits per second on non-coax cable. AppleTalk is the network language, LocalTalk is the actual cabling joining the computers. AppleTalk has certain advantages of simplicity, with compromises in speed.

ATM: Asynchronous Transfer Mode, the means by which data get transferred fast on the fiber-optic network itself, at a speed of 155 Mbps or higher. This is the very-high-volume data stream or "water main" that local

networks will tap into via the IDF's (Intermediate Distribution Frames, aka "telephone closets") and ADF's (Area Distribution Frames, the large-scale network nodes that form the backbone system). Highly touted at the beginning of the UCDavis Network 21 infrastructure improvement project, ATM turns out to be an expensive and possibly unworkable solution to campus backbone problems.

backbone: the interconnecting "wiring" (fiber optic in Network-21, combo of coaxial cable and some fiber optic in the current configuration) that allows networked computers to communicate with each other, share printers and other resources, and connect with the Internet at large; on our campus in 1996 the term refers both to existing backbone which is called UCDNet (mostly at 10BASE-T speed), and also Net21 high-speed version. Note that a subnet or LAN has a backbone as well; perhaps "spinal cord" would be more accurate anatomical analogy.

bandwidth: a measure of data density or capacity, how much "space" a signal or bunch of data takes up on a cable or fiber-optic line; video and sound are high-bandwidth modes, text a low-bandwidth one. The same cable that can carry hundreds of text messages at once will slow down trying to carry real-time video conferencing.

CD-ROM jukebox: Device for making the contents of many CD-ROMs available to remote sites over the network; for example the library is making more and more databases available over networks through CD-ROM, some of which require passwords and some not. The access time is relatively slow, but the storage capacity is huge.

classroom server: computer and hard-drive providing storage for class files and programs in a local computer classroom network, connected together through IT-Lab Management's classroom backbone..

closet: common term for IDF (Intermediate Distribution Frame), the physical location of switching computers called "hubs," which distribute data via designated "ports" to individual IP-addressed equipment in offices, labs and workrooms. Data streams come in over fiber-optic line and get parcelled out (routed) within the building over 10BASE-T wiring.

coax: (co-ax, short for coaxial cable)--a type of cabling with a conductor inside a braided-wire shield, arranged co-axially rather than side-by-side as in twisted-pair cabling such as 10BASE-T. Coax or Thin-net is more expensive to install and is being phased out.

configuration: the physical and electronic arrangement of equipment (hardware and software) that allows for successful work, especially for interchange of data over communications lines.

desktop computer: generic term for personal computer (Mac or IBM) in an office or home, as opposed to a special-purpose computer like a server or router or workstation, or a laptop or notebook machine.

domain: a defined Internet location or set of addressable computers, usually indicated in the last parts of an Internet address; for example the ucdavis.edu part of the hierarchical designation like fzstenze@peseta.ucdavis.edu, with the .edu signifying a US educational domain; company domains are designated with .com (as in timewaste.com), organizations with .org (as in dogooders.org).

domain restriction: the condition whereby some part of a network (e.g., a web server or special-collections CD-ROM) is accessible only via computers within a particular range of IP numbers; domain restrictions; become a problem when students and faculty use ISPs (Internet Service Providers, which have non-UC Davis domains) for Web access, and find themselves cut off from servers.

DNS (Domain Name System): naming conventions (including 4-part "dotted quad" version as well as text name) for hooking a server into the big network and making sure it can be addressed. For example, UCD's "bullwinkle" server is a domain known by the IP address 128.120.8.167 in machine-talk; the "peseta" mail server is 128.120.2.149. When a Web browser like Netscape cannot find a particular host computer's location (or if the host doesn't answer) the error message includes "cannot locate DNS."

DNR (Domain Name Resolver): a piece of software living in a Mac's System Folder that helps "resolve" domain names into machine-comprehensible form; you will not know this item exists until something goes wrong with it, in which case you will get the an error message referring to "Domain Name Reslover" (yes, with the picturesque typo there).

emulation: behavior like another type of entity, usually as in "terminal emulation." Terminal emulation software such as Kermit, ZTerm or ProComm allows a desktop computer to emulate (act like, display data from, interactively log in to) a terminal on a multi-user server-computer in a remote location, over phone lines via modems at both ends, or via hardwiring.

Ethernet: networking solution developed by Xerox, now the standard 10-Mbps way for computers to talk to each other; used to require coax cable, but with 10BASE-T can use twisted-pair. Ethernet is a protocol, a language and set of conventions for sending data; in common usage it also designates the concept of "hard-wired" as opposed to modem-and-phone-line access.

Ethernet card: add-on circuit board that plugs into the parallel port on the back of a computer, and allows high-speed data communication via 10BASE-T.

Ethernet-ready: able to receive 10BASE-T cabling directly into back of computer, with card and socket and software built in and not added-on.

Ethernet port: a cable jack or socket allowing a user to plug in an Ethernet-ready notebook computer and gain Internet access; the library is adding Ethernet ports, as are other areas on campus, although the process of configuring IP addresses and protocols is still being streamlined so that non-experts can do it easily.

EtherTalk: AppleTalk protocol running on an Ethernet network, allowing Macintosh computers to share printers within a subnet over the same lines that connect them to the Internet at large.

Eudora: e-mail-box program running on desktop computers featuring efficient use of mail server resources. Properly configured for a particular user, Eudora automates the process of dialing up to the campus mail server, logging in, and retrieving e-mail, and stores the e-mail files on the desktop's hard drive rather than on the IT server's storage. Because it downloads all incoming mail at once and then breaks the connection, Eudora can ease load on multi-user servers and modem banks; mail replies can be sent in a group just before the Eudora session concludes.

fiber-optic cable: fine spun-glass cabling that transmits data using laser pulses / light flashes; more efficient than metallic wire or coaxial cable, and used wherever the need for high-quality high-speed transmission justifies the higher costs. Network 21 as a whole differs from previous UCD networks in its commitment to ultra-high-speed fiber-optic cable between each building's router, and 10BASE-T connections between offices and a given building's hubs. The "quality" of a connection, the limits it places on bandwidth, can limit the types of data exchanged over a net: pictures that take minutes to load over phone-and-modem appear quickly over 10BASE-T; however, video images move slowly on 10BASE-T, and can be effective with the higher-speed 100BASE-T connections.

gateway / router: in physical sense, a special-purpose server or switching computer, joined to the high-speed network, having a DNS of its own; used, for example, between a departmental network (a subnet) and the campus network. Data would travel within the English subnet in Voorhies unless it is addressed to a DNS destination outside the subnet; the router would send it to the UCDNet, and another router sends it from there onto the broader Internet. "Gateway" is the concept, the idea of the place where one computer or group of computers joins the network, not the actual physical object; gateway can also be the point of entry between the general public and the Internet, so America On-Line is a gateway. Technically, a gateway routes data of different protocols, incorporating a translation step (for example, America On-Line's proprietary e-mailer gets translated into Internet-speak), whereas a router works with only one protocol. See also definition of router.

hard-wired: permanent high-speed connection to Internet, as opposed to modem-and-phone-line connection. Hard-wiring requires infrastructure in office (including NAM's (wall jacks), cabling, hubs in the building, and appropriate hardware in the desktop computer itself.

host: computer (or server) that can connect *as a computer* to other computers on the Internet, and identifiable as such through IP address. Note that this isn't the same as your PC connecting *as a terminal* to a server. Hosts require DNS addresses so that TCP/IP can find them. When you log in to a host like dale or chip, you are simply a "dumb" terminal on that multi-user server, and share its IP address with many other users, using it to send e-mail or perform other operations, with the waiting-time usually not very noticeable to you.

hub: switching computer located in IDF "closet," joining a local network or a building to the backbone via a router / gateway; hubs join to network devices by means of "ports," each able to serve an IP address. Departments in buildings with excess hub capacity can add devices by having IP addresses switched on; when all of a hub's ports are occupied, further expansion requires installation of another hub in the closet. Hubs, like other switching units, don't have hard-drive storage the way regular computers do, but pass off information packets very rapidly, as in a super-efficient mailroom.

Intermediate Distribution Frames (IDF's): "telephone closets" or substations, akin to the telephone cabinets currently in use, but beefier; when we want to activate a NAM, we will call a service person from IT and this person will throw the switches that give that NAM an address, just as we activate a phone number nowadays on an existing phone jack by calling the phone service.

IP number or IP address: the electronic address of any Internet site, usually expressed as a four-part decimal or "dotted quad" like 128.120.8.167, which is machine-talk for the UCDavis server better known as Bullwinkle. Most human interaction with Internet addresses takes place via their domain names (e.g., Bullwinkle). See also DNS and address.

Internet Service Provider (ISP): A for-profit provider of equipment and software furnishing Internet access, usually for a monthly fee. ISP's have purchased modem banks and run servers, but lease space on digital fiber-optic data trunk lines from firms like MCI and Sprint.

LAN: see Local Area Network.

local: in close physical proximity and joined together, but may be joined to a wider area network via some sort of server or router /gateway. A relative term, since UCDNet as a whole is a "local" network relative to the Internet as a whole, but the Olson computer classroom is a Local Area Network (LAN) relative to UCDNet.

LocalTalk: the cabling / connection apparatus joining Macintoshes on a LAN running AppleTalk networking protocol; will probably become obsolete as buildings move to Ethernet connections and the TCP/IP protocols.

Local Area Network (LAN): a group of interconnected computers or devices joined electronically, usually by wiring; may be designated as a subnet of a larger network like UCDNet, and may have its data stream organized or controlled by a local server / computer. LAN's may simply facilitate printer-sharing by several computers, or can be larger-scale conglomerations like the computer classrooms and other groups.

MacIP--Macintosh Internet Protocol: program or network language allowing a Macintosh to communicate with a local Ethernet and hence the Internet at large, and exchange files etc more easily and directly than terminal-emulator programs like Kermit do; requires an Ethernet-speed connection.

MacTCP: Macintosh implementation of TCP/IP, superseded on Power Macintoshes by Open Transport; a control panel on 68- series Macs where network connection details can be changed.

modem: device that allows a desktop computer to communicate over standard phone lines with another

computer or log in remotely to a server/host, usually at speeds ten times slower than Ethernet; requires another modem on the other end (the modem bank at the end of a dial-up number) to complete the connection. "Modem" is short for "modulator-demodulator," which refers to the process of translating computer data into serial phone-line-compatible form and then extracting it again on the other end. A modem is to computers what a phone is to humans: to communicate you need one on each end, with wiring and switching in between.

modem bank: set of modems connected to a server, furnishing each remote user a temporary connection to a campus computer, either as an IP-addressed Internet machine (using a PPP or SLIP line), or as a terminal to a multi-user host (using a POP connection). The UCD modem bank has mushroomed over the past several years, but the demand for outside modem access still exceeds supply, especially at peak periods. Most modem banks typically have a single phone number with a switch to roll calls down the bank: you dial 752-7900 as the point of entry but may be automatically rolled over to (say) 752-7985 or any available modem number.

modem initialization string: a set of cryptic letters and numbers such as "AT&0" that a particular brand of modem needs in order to communicate successfully with a network. The only time you learn about modem inits is when you buy a new modem or card, or install communications software that won't run with the default string.

modem speed: the approximate number of bits-per-second (bps) that a given connection can accommodate; phone lines limit the effective speed of a modem to between 14400 and 28800 bps; if the fiber-optic cable is a huge water main of data, the phone line is a small garden hose.

NAM--Network Access Module: the special jack or module that connects a computer or other networked device to the office cabling that leads to the port that joins to the hub that links with the router that goes through the gateway that merges onto the Network 21 trunk fiber-optic cable that lives in the house that Jack Peltason built (sorry). Cost: none given, but IT tells us to anticipate an activation cost of ~$60 per hookup plus possibly a service fee.

network: strictly speaking, any group of interconnected computers or peripherals--a computer connected to a printer is a simple network, with the data stream travelling over the network cable through the computer's printer port. More commonly, a network joins multiple computers and peripherals (e.g., to share laserprinting); a network can also join networks together, as in UCDNet or the amorphous aggregation known as the Internet.

port: point of entry / exit for a data stream, either at the back of a computer, or (in the network sense), for wiring from a desktop's IP address to a hub in an IDF closet; each hub generally serves 12 or 24 ports. Activating another IP address in a local network may be as simple as throwing a switch (if a port is free) or as complex as buying and hooking-up a whole new hub if no ports are left.

POP--Post-Office-Protocol: the mode of connecting to a large multi-user server (like chip, dale, etc) and extracting mail or other information. You go to a window (a dial-up line) and a clerk helps you, fetching mail or whatever; the clerk may be helping lots of people so your service may be slow.... Currently modem access to e-mail servers is through POP connections, but your login only fetches mail from the POP server to another machine; you do not log in directly to a POP machine.

POP--Point of Presence: physical manifestation of a digital trunk line in a geographical location, vital to efficient operation of independent Internet Service Providers. In Davis, for example, which because of its essentially rural nature does not have a concentration of big network lines from Pac Bell or MCI or others, an ISP must take a rather circuitous route from analog to digital and back, rendering connections less efficient.

PPP--Point-to-Point Protocol: a type of dial-in modem connection that establishes a direct IP-addressed Internet connection, instead of a terminal connection to a single multi-user host. Users with PPP or SLIP connections can run Netscape or other Web browers, unlike users with terminal connections; with a PPP or SLIP connection the processor in your desktop computer is more actively involved in manipulating the data from the network, instead of just passively receiving and displaying it.

protocol: the network-communication program or language that allows computers to reliably exchange information, electronic packet by labelled packet. Usually transparent to users, in that we don't know whether our message has been sent using MacIP or some other Internet Protocol, so long as it gets to its destination in the right format. A subnet running one protocol can interact with another net running a different protocol as long as there's a gateway making the speedy translation and routing decisions.

router / gateway: The IT literature blandly calls this a "box," but this device is a special-purpose switching computer specifically dedicated to managing network traffic; the router isolates LAN traffic from the backbone / Internet at large, unless there's a reason for going outside the system. Routers don't have storage drives, but just fling message packets back and forth, usually with the same protocol. By analogy to the campus mail system, a router is the sorting room over at Mail Services, where mail to another department stays within the subsystem, and mail going off campus goes to US Mail; in this analogy the mailroom is both a router (same protocol, on campus) and a gateway to a different protocol (stamped US Mail).

server: computer dedicated to interact with other networked computers to share resources (files, printing capabilities, a modem bank); depending on scale can be anything from a garden-variety PC or Mac to a very-high-power Sun Microsystems or SGI workstation serving hundreds of remote terminal connections the way chip, dale, and rocky do. Computer classrooms have their own servers providing storage for class files and programs.

SLIP--Serial Line Internet Protocol: dial-up Internet connection like PPP allowing Web browsing etc, with temporary IP address, over phone lines.

SMTP--Simple Mail Transfer Protocol:

SunServer: powerful workstation computers built by Sun MicroSystems, able to serve hundreds of users at a time via dial-up and hard-wire connections.

TCP/IP: Transmission Control Protocol / Internet Protocol--the language spoken on the Internet, a set of standard protocols allowing communication to computer "hosts" on different nodes of a local network, across the nation and worldwide.

telephone closet: see closet: physical location of IDF switching computers.

terminal: point of entry to a multi-user server like dale or chip or bullwinkle; terminal-emulator programs (e.g., Kermit, ZTerm, ProComm) allow individual computers to connect to servers and manipulate mail or read news without actually interacting as equals; for example, the mail you read using the Pine program doesn't actually reside on your desktop computer until you execute the commands that move it over to your physical location. With full Ethernet connections the interactions will be tighter and more flexible: an instructor in Voorhies could leave the office computer on and log into it from home, and thence move around the network backbone (including the classroom servers) with ease.

terminal emulation program: software like Kermit or ZTerm run on a desktop computer, allowing it to interact with a multi-user server via modems. See emulation.

thin-net: a less expensive variety of coaxial-cable Ethernet hook-up.

UCDNet: the current Ethernet-speed network backbone connecting the UCD campus with the Internet at large, in place since the mid-late 1980's; some parts of UCDNet are now connected with fiber-optic cabling, but Network 21 plans call for full fiber-optic connection.

Unix: the versatile, powerful, but notoriously user-hostile operating system environment running on most networks, allowing multiple users and multiple programs to run simultaneously on the same powerful

computers. Menu-driven application programs like Pine insulate users from the Unix interface, although these programs are often launched from the Unix "system prompt," a $ or % sign.

Web server: a computer running Web server software and permanently connected to the Internet, dedicated to maintaining web pages on its hard drive; accessible from outside via Internet protocols, hence must have its own DNS address, and thus physically have its own NAM-->port-->hub-->router connection.

workgroup server: powerful computer dedicated to performing network tasks like printing, file storage, Web page storage, etc; each computer classroom has its own workgroup server, parts of which are accessible from the individual student computer stations.

workstation: depending on context, generally a very powerful and fast computer (single-user or multi-user) that can connect to a network and perform functions more advanced than those of dumb terminals; workstations may be without their own hard drive storage units, and less robust computers can be called workstations as well. Workstations employed as servers may serve dozens or hundreds of remote terminals, as is the case when users log in to SunServers like chip, dale, and the like, and run Unix programs like Pine. To compound confusion even further, "work station" in a generic sense connotes a person's work space, his/her computer and desk....

E-mail comments or suggestions.

Return to Computers in Composition Home Page

Return to John Stenzel's Home Page